SpringerBriefs in Computer Science

SpringerBriefs present concise summaries of cutting-edge research and practical applications across a wide spectrum of fields. Featuring compact volumes of 50 to 125 pages, the series covers a range of content from professional to academic.

Typical topics might include:

- A timely report of state-of-the art analytical techniques
- A bridge between new research results, as published in journal articles, and a contextual literature review
- A snapshot of a hot or emerging topic
- An in-depth case study or clinical example
- A presentation of core concepts that students must understand in order to make independent contributions

Briefs allow authors to present their ideas and readers to absorb them with minimal time investment. Briefs will be published as part of Springer's eBook collection, with millions of users worldwide. In addition, Briefs will be available for individual print and electronic purchase. Briefs are characterized by fast, global electronic dissemination, standard publishing contracts, easy-to-use manuscript preparation and formatting guidelines, and expedited production schedules. We aim for publication 8–12 weeks after acceptance. Both solicited and unsolicited manuscripts are considered for publication in this series.

**Indexing: This series is indexed in Scopus, Ei-Compendex, and zbMATH **

More information about this series at https://link.springer.com/bookseries/10028

Youyang Qu · Longxiang Gao · Shui Yu ·
Yong Xiang

Privacy Preservation in IoT: Machine Learning Approaches

A Comprehensive Survey and Use Cases

Springer

Youyang Qu
Data61
Australia Commonwealth Scientific
and Industrial Research Organization
Melbourne, VIC, Australia

Shui Yu
School of Computer Science
University of Technology Sydney
Ultimo, NSW, Australia

Longxiang Gao
Shandong Computer Science Center
Qilu University of Technology
Shandong, China

Yong Xiang
School of Information Technology
Deakin University
Burwood, VIC, Australia

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-981-19-1796-7 ISBN 978-981-19-1797-4 (eBook)
https://doi.org/10.1007/978-981-19-1797-4

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

Internet of Things (IoT), as a booming computing architecture, is experiencing rapid development with a speed beyond imagination. Nowadays, IoT devices are so pervasive that they have become key components of human daily life, such as sensors, intelligent cameras, smart wearable devices, and a lot more. By reshaping the existing network architecture, IoT has provided significant convenience and improvement of quality of life.

Since IoT devices are deployed ubiquitously, an increasing volume of data is collected and transmitted over IoTs. The statistic shows total data volume of connected IoT devices worldwide is forecast to reach 79.4 zettabytes (ZBs) by 2025. However, the data privacy issues become even severe because sensitive information of collected data is not properly managed, especially health data, location data, identity-related data, etc. Moreover, data from multiple sources pose further challenges since the interconnections among the data may reveal more sensitive information. Furthermore, the advancement of data pattern extraction and data analysis techniques put privacy under more serious threats. Thus, privacy preservation has become a crucial issue that needs to be well considered in this age of IoT.

Machine learning has proved its superior performance in data manipulation field. In addition to perform predictive analysis or optimization-oriented services, machine learning algorithms are adopted in privacy-preserving data sharing and publishing scenarios. It attracts extensive interest from both academia and industry. Among all existing solutions, reinforcement learning, federated learning, and generative adversarial networks (GAN) are the most popular and practical ones. Extensive research has been conducted to leverage or modify them for privacy protection considering diverse conditions. Therefore, they are also the main focus of this monograph, through which the rationale of machine-learning-driven privacy protection solutions are present.

In this monograph, we are going to comprehensively and systematically introduce machine-learning-driven privacy preservation in Internet of Things (IoTs). In this big data era, an increasingly massive volume of data is generated and transmitted in IoTs, which poses great threats to privacy protection. Motivated by this, an emerging research topic, machine-learning-driven privacy preservation, is fast

booming to address various and diverse demands of IoTs. However, there is no existing literature discussion on this topic in a systematical manner. The authors in this monograph aim to sort out the clear logic of the development of machine-learning-driven privacy preservation in IoTs, the advantages, and disadvantages of it, as well as the future directions in this under-explored domain. The issues of existing privacy protection methods (differential privacy, clustering, anonymity, etc.) for IoTs, such as low data utility, high communication overload, and unbalanced trade-off, are identified to the necessity of machine-learning-driven privacy preservation. Besides, the leading and emerging attacks pose further threats to privacy protection in this scenario. To mitigate the negative impact, machine-learning-driven privacy preservation methods for IoTs are discussed in detail on both the advantages and flaws, which is followed by potentially promising research directions.

The prominent and exclusive features of this book are as follows:

- Reviews exhaustive the key recent research into privacy-preserving techniques in IoTs.
- Enriches understanding of emerging machine learning enhanced privacy-preserving techniques in IoTs.
- Covers several real-world applications scenarios.
- Maximize reader insights into how machine learning can further enhance privacy protection in IoTs.

This monograph aspires to keep readers, including scientists and researchers, academic libraries, practitioners and professionals, lecturers and tutors, postgraduates, and undergraduates, updated with the latest algorithms, methodologies, concepts, and analytic methods for establishing future models and applications of machine-learning-driven privacy protection in IoTs. It not only allows the readers to familiarize with the theoretical contents but also enables them to make best use of the theories and develop new algorithms that could be put into practice.

The book contains roughly three main modules. In the first module, the book presents how to achieve decentralized privacy using blockchain-enabled federated learning. In the second module, the personalized privacy protection model using GAN-driven differential privacy is given. In the third module, the book shows the hybrid privacy protection using reinforcement learning. Based on the above knowledge, the book presents the identified open issues and several potentially promising future directions of personalized privacy protection, followed by a summary and outlook on the promising field. In particular, each of the chapter is self-contained for the readers' convenience. Suggestions for improvement will be gratefully received.

Melbourne, Australia — Youyang Qu
Shandong, China — Longxiang Gao
Ultimo, Australia — Shui Yu
Burwood, Australia — Yong Xiang

Acknowledgments

We sincerely appreciate numerous colleagues and postgraduate students at Deakin University, Melbourne and University of Technology Sydney, Sydney, who contribute a lot from various perspectives such that we are inspired to write this monograph. We would like to acknowledge the support from the research grant we received, namely, ARC Discovery Project under the file number of 200101374. In this book, some interesting research results demonstrated are extracted from our research publications that indeed (partially) supported through the above research grants. We are also grateful to the editors of Springer, especially Dr. Nick Zhu, for his continuous professional support and guidance. Finally, we would like to express our thanks to the family of each of us for their persistent and selfless supports. Without their encouragement, the book may regrettably become some fragmented research discussions.

Melbourne, Australia — Youyang Qu
Shandong, China — Longxiang Gao
Sydney, Australia — Shui Yu
Melbourne, Australia — Yong Xiang
December 2021

Contents